April 2024

Expert Insights
PERSPECTIVE ON A TIMELY POLICY ISSUE

MAREK N. POSARD, TODD C. HELMUS, MICHELLE WOODS, BILVA CHANDRA

The 2024 U.S. Election, Trust, and Technology

Preparing for a Perfect Storm of Threats to Democracy

The 2020 U.S. presidential election was mired in controversy and conflict. Foreign governments interfered in the election, while some domestic leaders alleged election fraud before voting even began (Inskeep, 2021; Marcellino et al., 2020; Posard et al., 2020). After the election, assertions that the election was "stolen" gained so much traction that, as the certification process got underway, a crowd gathered for a rally in Washington, D.C., and subsequently turned violent, attacking the U.S. Capitol and causing injuries and deaths, including to law enforcement officers defending the building (Select Committee to Investigate the January 6th Attack on the United States Capitol, 2022). In the months and years since then, messages discrediting the election results and the agencies and officials involved in investigating the riot and election-related charges have continued unabated, particularly on social media (Sullivan, 2023).

These events further eroded many Americans' trust in U.S. elections. One survey—conducted more than two years after the 2020 election—showed that 30 percent of Americans believed that President Joe Biden won the 2020 elec-

We focused on vulnerabilities associated with three types of assets required for fair, democratic elections: physical assets, such as voting machines; human assets, such as election officials; and reputational assets, such as public confidence in elections.

tion because of voter fraud (Monmouth University Polling Institute, 2023). As the United States prepares for the 2024 presidential election, these familiar messages could resurface, new sources of falsehoods could emerge to challenge the credibility of the U.S. election system, and new technologies—including artificial intelligence (AI)—could enable efforts to undermine confidence in the results.

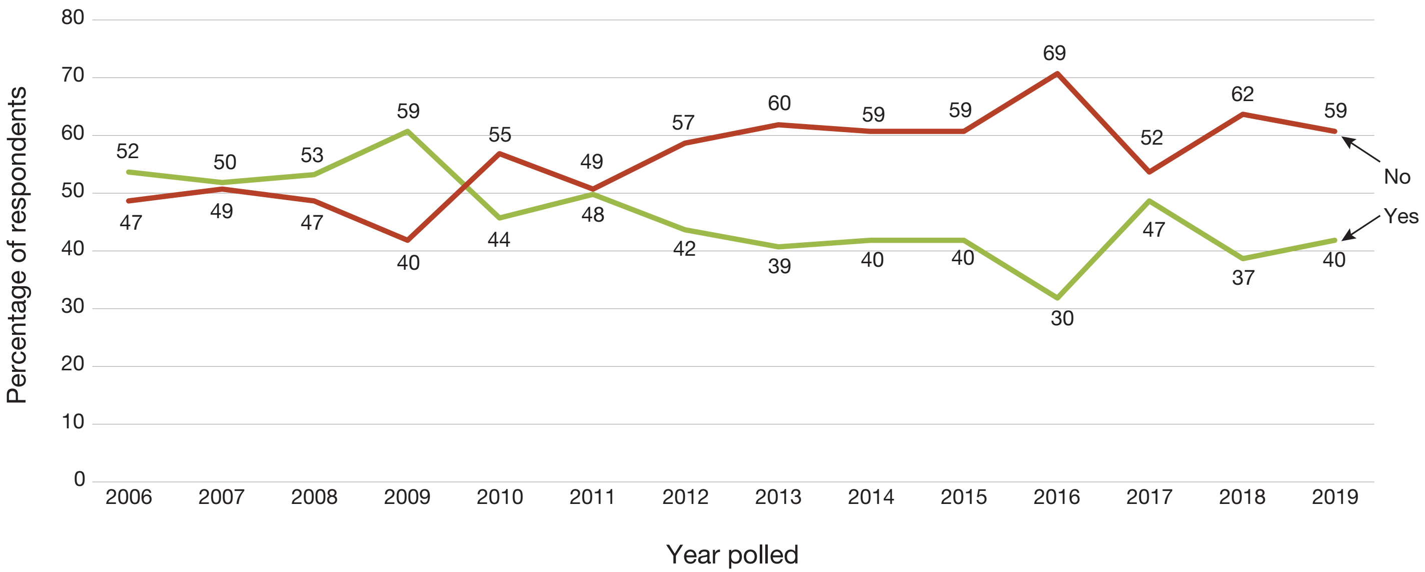
The RAND Homeland Security Research Division commissioned work to identify key risks and prepare for potential threats from those risks in advance of the 2024 U.S. presidential election. We explored a set of key risks for which federal, state, local, tribal, and territorial officials should prepare in the lead-up to future elections, particularly the 2024 U.S. presidential election. We focused on vulnerabilities associated with three types of assets required for fair, democratic elections:

- physical assets, such as voting machines
- human assets, such as election officials
- reputational assets, such as public confidence in elections.

Although threats to any election-related assets could undermine the credibility of U.S. elections, there is the prospect of a perfect storm in which several seemingly unrelated threats target these assets simultaneously. The purpose of this paper is to organize the key features of this perfect storm, explore how recent advances in generative AI could accelerate the storm's effects, and discuss next steps for policymakers and other stakeholders to consider when preparing for these threats to the 2024 presidential election.

The Growing Partisan Divide in Public Confidence in U.S. Elections

The figure on the next page tracks responses over time to the question, "In this country, do you have confidence in each of the following, or not? How about honesty of elections?" (Reinhart, 2020). From 2006 to 2008, response patterns tended to be evenly split between "yes" and "no." After 2011, responses diverged into their current pattern, Public Confidence in the Honesty of U.S. Elections, 2006–2019



SOURCE: Adapted from Reinhart, 2020.
NOTE: The question read, "In this country, do you have confidence in each of the following, or not? How about honesty of elections?

with a majority of respondents reporting that they were not confident in the honesty of U.S. elections.

Furthermore, additional Gallup survey data show that, during George W. Bush's presidency, in 2006, 92 percent of Republican respondents reported being very or somewhat confident in the accuracy of the outcome of U.S. elections (the highest for either party in all polling years), compared with 66 percent of responding Democrats. During Barack Obama's presidency, in 2016, 55 percent of Republican respondents reported confidence in election accuracy, versus 85 percent of responding Democrats. In 2022, the midterm year following the contentious 2020 election, just 40 percent of Republican respondents reported confidence in the accuracy of elections, while confidence among responding Democrats was higher than in any other year of the poll, at 85 percent. These examples highlight a link between claims challenging election integrity and partisanship views (McCarthy, 2022).

With these partisan trends in mind, we explored threats to past U.S. elections, the consequences, and potential vulnerabilities could be exploited in 2024. Later in this paper, we present a series of notional scenarios that could serve as the basis for exercises as election officials assess future risks and prepare to mitigate them.

Key Election Assets as Points of Vulnerability

An election is an "act of selecting a person to fill an office" (National Conference of State Legislatures, undated). Broadly speaking, successful elections are those that reflect the free expression of the will of the public (U.S. Agency for International Development, undated). This definition of *success* includes elections that are freely accessible to the public and maximize participation by all subgroups, with a process and outcome that are objectively fair, and with broad public acceptance of the outcome.

To help clearly organize the various types of risks to elections—and the intersection of these risks—we developed a taxonomy that focuses on three types of assets required to hold a successful election. The table profiles these three classes of assets—and the individual components that could be vulnerable to future attacks—in more detail.

Physical assets are election-related resources that can be seen and touched (see, e.g., Hodgson, Brauner, and Chan, 2020), human assets are the people involved in carrying out these elections, and reputational assets are public perceptions of these physical and human assets (Kavanagh, Hodgson, and Gibson, 2020). Because the United States has a decentralized election system, most physical and human assets are managed by local and state governments.

A key argument we make here is that how election assets are managed in one jurisdiction could affect reputational assets for elections within the same state or across the country.

Taxonomy of Key Election Assets, with Examples

Asset Class	Definition	Example
Physical	Any facility, equipment, information storage system, or process that supports the act of voting and the recording of votes in an election	Physical space (e.g., voting center, precinct) Voting machine Computer system Ballot Voter registration lists and databases
Human	Any person with official duties pertaining to some part of the election process	Federal, state, or local election employee Government contractor Nongovernment partner Volunteer poll worker
Reputational	Public perceptions of the physical and human assets involved in an election, as well as confidence that the outcome was fair	Perception about the frequency of voter fraud Accuracy of vote-counting Overall ballot security (e.g., mail-in or in-person ballots)

NOTE: The definitions of *physical*, *human*, and *reputational* are ours, informed by key literature (Hodgson, Brauner, and Chan, 2020; Kavanagh, Hodgson, and Gibson, 2020). These asset classes are not necessarily mutually exclusive, but this taxonomy provides a useful starting point for understanding the pathologies of risks to actual or perceived election integrity.

Recent Claims Challenging U.S. Election Integrity

The 2024 U.S. election is not the first to involve popularized claims about U.S. election integrity. This section describes some of the more popular claims, dating back to 2000. Earlier in this century, many of the claims challenging the integrity of U.S. national elections focused on threats to physical assets. For example, following the 2000 presidential election, results in several counties in Florida came under scrutiny in response to concerns about irregular ballot-counting, ending in a U.S. Supreme Court decision to stop a recount in the state that decided that election (Elving, 2018). Some made claims about irregularities with electronic voting equipment in Ohio during the 2004 presidential election ("Machine Glitch Gave Bush Extra Ohio Votes," 2004).

During the 2008 presidential election, attention focused on human assets—namely, nongovernment officials working to improve voter turnout. For example, Republican presidential candidate John McCain raised concerns about voter fraud by the now-defunct Association of Community Organizations for Reform Now (ACORN), which worked to mobilize voters in low-income and other underrepresented communities (Seelye, 2008). In the lead-up to the 2016 presidential election, the scope of claims about risks to U.S. elections broadened to include not only physical and human assets but reputational assets as well, with then-candidate Trump sounding an alarm about the prospect of a "rigged election" (Collinson, 2016).

The 2020 election is the most recent presidential election in the United States—and claims of election fraud continue to circulate four years later (e.g., Fung, 2023). To avoid delving into partisan divides, we focus our discussion on claims that resulted in filings in state or federal courts under penalty of perjury. This last presidential election culminated in claims of election fraud, punctuated by false statements that votes were altered via cyberattacks on voting machines manufactured by Dominion Voting Systems (physical assets); false claims of election fraud committed by election officials and subsequent harassment of those officials (human assets); and continued unsubstantiated claims of systemic oversight failures during the election (reputational assets), including allegations that mail-in ballots were uniquely vulnerable to tampering (physical assets). It remains to be seen how major court cases on these matters will affect political rhetoric in 2024 (see *Freeman v. Giuliani, 2022*; Sullivan, 2023; *US Dominion, Inc. v. Fox News Network, Inc.*, 2023).[1] In the next section, we explore major court cases in the aftermath of the 2020 election and their resulting criminal and civil penalties.

Cases About Threats to U.S. Elections

Multiple threats to physical, human, and reputational election assets during the 2020 U.S. presidential election resulted in cases filed in state and federal courts. We focus on court cases because the person filing must submit facts to support their claims under penalty of perjury. Thus, these cases provide a clearer record of claims and the degree to which they are substantiated than other claims.

Cases Related to Physical Assets

Some of the popular false claims in 2024 focused on voting systems manufactured by Dominion Voting Systems. Such false claims included statements that Dominion changed or deleted votes; that prominent family members of Democratic politicians had ownership stakes in the company; that federal entities, including the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the Central Intelligence Agency, had missions to commit voter fraud; and that software updates conducted the night before the 2020 presidential election might have altered the count. Dominion ultimately settled its defamation suit against Fox News for $787 million (*US Dominion, Inc. v. Fox News Network, Inc.*, 2023); litigation against Newsmax and One America News was still pending at the time of this writing. Separate defamation lawsuits against Newsmax and One America News by a former Dominion executive who was forced into hiding after receiving death threats were settled in April 2021 and September 2023, respectively (Shamsian, 2023). Smartmatic, another manufacturer of voting systems, continues to pursue similar lawsuits against Fox News and Newsmax as of October 2023.

Cases Related to Human Assets

In 2020, some raised U.S. election security concerns that focused on human assets. For example, Ruby Freeman and Wandrea ArShaye "Shaye" Moss served as official election workers in Georgia during the 2020 presidential election. They became targets of false accusations of election fraud, resulting in ongoing harassment from members of the public. These false claims included accusations of introducing large numbers of illegal ballots during the counting of legitimate ballots, counting the same ballots multiple times, using data storage devices to illegally access Dominion voting machines, and otherwise participating in a criminal enterprise to commit voter fraud (*Freeman v. Giuliani*, 2022). Freeman and Moss sued former President Trump's attorney Rudy Giuliani for defamation, intentional infliction of emotional distress, and civil conspiracy to commit those two torts, and a default judgment was entered against Giuliani, with punitive and compensatory damages awarded.

Cases Related to Reputational Assets

During the 2020 presidential election, then-President Trump claimed that outcome-determinative fraud was occurring. After he lost the election, he continued making claims about election fraud and, in August 2023, was indicted on charges of conspiracy to defraud the United States, conspiracy to obstruct an official proceeding, obstruction and attempted obstruction of an official proceeding, and conspiracy against rights, all in relation to attempting to overturn the results of the 2020 presidential election (*United States of America v. Donald J. Trump*, 2023). To date, these cases are still pending without legal judgment.

Some examples of this alleged criminal conspiracy include purported attempts to get election officials to change electoral votes; organizing slates of fraudulent electors in several states; using the U.S. Department of Justice to investigate unsubstantiated allegations of election crimes; and interfering with the election certification process in Congress, including by provoking the attack on the U.S. Capitol. A grand jury indicted former President Trump in August 2023, during the early stages of the Republican primary season.

The Evolution of Artificial Intelligence–Related Threats to U.S. Elections

Although physical and human election assets have been threatened directly, reputational attacks in the less direct form of mis- and disinformation are a common thread in litigation. In prior research, we examined patterns of social media traffic and identified sources of foreign interference in the run-up to the 2020 presidential election (Marcellino et al., 2020). These efforts have had the dual effects of sowing confusion among the U.S. public about what is and is not true and undermining confidence in elections and, indeed, democracy.

AI-enabled platforms could pose a new set of challenges to ensuring public confidence in U.S. institutions. Examples include the following:

- **new capabilities from AI:** These technologies can generate text and realistic but fake photographic images, audio, and video, and they have the potential to significantly increase the persuasive power of disinformation (Helmus, 2022; Marcellino et al., 2023).
- **scalability of use:** Both foreign and domestic actors can use large language models (LLMs) to quickly and easily generate persuasive text to populate social media posts, news articles, personal blogs, or discussion boards. With AI, this content can be drafted at scale to support large-volume social media campaigns.
- **ease of concealing the producing source:** Foreign governments—especially those lacking large cadres of proficient English speakers who are versed in American culture—will especially benefit from the ability to generate and disseminate messages that effectively obscure their foreign origins.

Several recent studies have highlighted the ease with which LLMs can be used to generate false content. For example, NewsGuard Technologies, which has developed a credibility scoring system for websites, asked the free AI system ChatGPT 3.5 to produce 100 false narratives from NewsGuard's catalog of Misinformation Fingerprints—a collection of data points used to track the spread of misinformation online. ChatGPT succeeded 80 percent of the time and produced what were described as "eloquent, false and misleading claims about significant topics in the news, including COVID-19 [coronavirus disease 2019], Ukraine and school shootings" (Brewster, Arvanitis, and Sadeghi, 2023). Several months later, NewsGuard repeated the test using Generative Pretrained Transformer (GPT) 4 and found that the new system produced false content 100 percent of the time and offered no disclaimers indicating that the information was false (Fischer, 2023).

Studies suggest that this generated content can be highly persuasive. Researchers from Georgetown and Stanford universities identified Russia- and Iran-authored propaganda about the Middle East and used its central ideas to generate related content using an LLM. They showed the simulated Russian and Iranian propaganda and the GPT-3 content to research participants and found that both significantly influenced participants' opinions (Jingnan, 2023). Another study compared tweets authored by humans and those authored by GPT-3, finding that research participants were 3-percent less likely to identify a tweet as false if it was AI generated than if it were written by a person (Williams, 2023).

AI can also be used to generate highly realistic audio recordings and photographic images. Generative AI platforms, such as DALL-E, Midjourney, and Stable Diffusion, have made headlines for their ability to generate realistic images based on simple text prompts. For example, in 2023, images falsely depicting scenes of former President Trump's arrest in New York briefly went viral, as did an image of an explosion at the Pentagon (Bond, 2023a). AI-generated images have already been used in political campaigns, including one that falsely depicted former President Trump embracing Anthony Fauci, then-director of the National Institute of Allergy and Infectious Diseases who was the target of efforts by right-leaning officials, media outlets, and social media accounts to undercut his recommendations for preventing the spread of COVID-19 (Bond, 2023b). Although some AI platforms prevent users from creating images of political leaders and other major public figures, studies suggest that they can easily be coaxed into producing content that supports various disinformation-based claims. Demonstrating this work-around, the tech company Logically, which specializes in designing AI solutions to prevent the spread of misinformation, showed that DALL-E 2, Midjourney, and Stable Diffusion accepted more than 85 percent of prompts to generate evidence for mis- and disinformation narratives, including those supporting election-interference claims (Walter, 2023). The generated images, albeit of low quality, showed people stuffing ballot boxes, tampering with election equipment, and stealing boxes of ballots.

Beyond spreading false information about elections themselves, AI will likely play a significant role in disrupting legitimate public debate on such issues as pregnancy termination, immigration, gun policy, and discrimination, which can galvanize some voters and demotivate others (Posard et al., 2020). With assistance from AI, both foreign and domestic actors will be able to target content to increasingly specific audiences at low cost and with minimal effort.

Overall, given the ease of use and the realism of AI-produced content, one can expect LLMs and image, video, and audio generators to increasingly become tools for perpetuating mis- and disinformation and stoking public support for false claims. Absent significant forms of government or industry self-regulation, the upcoming 2024 election will almost certainly not be spared, much less other elections: local, state, and nonpresidential national elections.

Notional Scenarios to Illustrate Potential Threats

We developed two notional scenarios to help federal, state, local, tribal, and territorial officials prepare to address potential threats to election assets as the 2024 presidential election approaches. The approach for developing these notional examples was purposefully broad. The first scenario starts with a foreign attack on U.S. election infrastructure; the second scenario focuses on a foreign attack on nonelection infrastructure in the United States. Each of these notional scenarios starts with a risk that could threaten one type of asset class, then introduces risks to other asset classes. These risks are based loosely on past events and were developed to showcase concerns about multiple election security–related risks occurring simultaneously. The purpose of these notional scenarios is to illustrate the ways in which different classes of threats are interrelated. Such examples can inform the types of scenarios developed for various election-related analytical gaming exercises designed to prepare for the 2024 presidential election.

The scenarios are intended to illustrate the conditions under which risks to one type of election asset could combine with risks to other types of assets, creating cumulative risks that could undermine public confidence in U.S. elections—and how AI can magnify these risks.

Although the scenarios are based loosely on public reports of past and projected threats to U.S. elections, they are *fictional* and are intended to highlight the cumulative impact of a contentious election cycle. They do not refer to real people or events and should not be interpreted as a prediction of what could happen in 2024 or at any other point in the future.

Scenario 1: Targeting U.S. Election Infrastructure

Russia Uses Hackers, Artificial Intelligence, and Astroturf Social Media Campaigns to Sow Doubt About Election Integrity

Polls show that Incum Bent, the Incumbent Party candidate, has a slight and growing advantage, and supporters of Chall Enger, the Challenger Party candidate, view such polls with growing skepticism. As a result of this skepticism, some vocal supporters of Enger express concern that the Incumbent Party will attempt to steal the election. Social media chatter grows louder with speculation that the Incumbent Party will try to rig the election in its favor.

The Russian government has been waiting for U.S. audiences to raise concerns about election fraud, and it sees this as its cue to execute a planned operation to sow confusion. In the first phase of this effort, Russian intelligence officials release a trove of emails stolen from Bent's campaign staff. Several months earlier, a Russian hacking group had accessed the email server. Most of these emails offer a banal view of day-to-day election activities, but Russian intelligence officials inserted several forged emails that appeared to show that Bent's election staffers had discussed ways to manipulate election results in the battleground states of Ohio and Pennsylvania. Slowly, news organizations begin to review and report on these emails, even though the Federal Bureau of Investigation concluded that they were fake. As real and false news reports about the hack is reported, Russian trolls based at the Internet Research Agency in St. Petersburg, Russia, begin the next phase of the operation. These trolls, who operate fake American social media accounts, use ChatGPT to craft authentic-looking English-language tweets publicizing news reports claiming that all the hacked emails are real and urge members of the Challenger Party to be on the lookout for election fraud.

A counter-disinformation research institution based in the United States publishes a report with evidence that the Russian-authored social media posts were part of a government-sponsored "astroturf" campaign on social media—that is, a social media operation that uses fake accounts to simulate authentic grassroots social media conversations, but the findings receive little attention on the social media platforms or from the public at large.[2]

Iran Compromises Voter Rolls and Disseminates Artificial Intelligence–Generated Imagery, Reinforcing Existing Doubts

Next, Iranian hackers worm their way into county-managed voter registration records in Ohio and state-managed voter registration databases in Pennsylvania.[3] After accessing these systems, the hackers selectively delete the records of about 20 percent of Challenger Party voters.

On Election Day, the U.S. public is already on edge because of increasing online chatter about election interference, with some voices being authentic and some not. As voters arrive at the polls, some Challenger Party voters in Pennsylvania and Ohio are informed that they are not on the voter rolls. They are encouraged to cast provisional ballots, and the counties plan to confirm their registration using backup records.[4] However, word spreads nationwide that Challenger Party voters are being turned away at the polls in record numbers. Both Iranian astroturf accounts and genuine Challenger Party accounts seize on this news and express alarm at the seemingly obvious signs of voting fraud. The story quickly gains traction, first on partisan news websites and then with more-traditional national outlets, such as *USA Today* and the *New York Times*. Election-night tallies of statewide vote counts suggest that Bent has the lead in votes—particularly in Ohio and Pennsylvania, with the caveat that a significant number of provisional ballots have yet to be confirmed in both states.

A grainy video surfaces online allegedly depicting election workers discarding ballots in a trash can in an unknown location. Accompanying posts allege that it depicts the destruction of Challenger Party votes at a vote-tallying center in Philadelphia, Pennsylvania. The video and posts quickly go viral. Soon, still photos of discarded Challenger Party ballots follow and fill the online space. They are complemented by purported eyewitness accounts of paper ballots being destroyed and election workers tampering with voting machines.

Questions to Consider

This notional scenario highlights some questions for election officials to consider, such as the following:

- How could the U.S. intelligence community best warn the American public about foreign actors trying to sow doubt about the 2024 election?
- How would state and local officials respond to safeguard elections if foreign actors did compromise their voter rolls?
- What actions should local, state, and federal election authorities take should candidates Bent and Enger pursue litigation about the 2024 election?

Scenario 2: Targeting Nonelection U.S. Infrastructure

Cyberattacks Target Vulnerable Critical Infrastructure

This notional scenario begins with an attack on nonelection infrastructure that decreases public confidence in the elections. Just days before voting begins, critical infrastructure is hit by a series of cyberattacks that target local governments' and utility companies' outdated computer systems (see Brumfield, 2019). Ransomware attacks shut down water and wastewater utilities serving Incumbent-leaning districts in two swing states (see Jaskolka, 2021, and Miller, 2021). As the outage wears on, store shelves are emptied of bottled water, local businesses are forced to close, officials hastily arrange for water supplies to be trucked in, and people with access to vehicles and alternative places to stay flee the area. For anyone who has not opted to receive a mail-in or absentee ballot, the deadline has passed to request one, and chances are good that they will not return to their precinct to vote before the voting deadline. Federal authorities suspect that a foreign adversary is behind these coordinated attacks, but, as yet, there is no proof to support this claim.

Because this attack targeted the water and wastewater utilities of swing states mere days before the national election, it is too late for election officials to mail paper ballots to the temporary addresses of voters who had planned to cast ballots in person but have left the area. In response, local officials request that Challenger Party–aligned governors allow these voters to cast provisional ballots in the districts where they are staying and allow additional time for their ballots to be counted. They also propose opening additional polling places to make it easier for those who did not the leave the area to vote in person. These voters tend to be in lower income brackets; furthermore, many of these remaining voters are Black and Hispanic.

After some delay, these initiatives are approved, and officials attempt to notify affected prospective voters of their options directly via phone calls, text messages, email, and social media and indirectly through press releases and announcements on their state and county websites. As these initiates are carried out, several partisan political action committees file lawsuits alleging election fraud. Federal courts will take months to decide these cases.

Online Social Media Campaigns Sow Confusion

As news spreads about the attacks and efforts to mitigate the effect on the upcoming election, social media platforms are flooded with speculation that the alleged cyberattacks were an "inside job," posts disparaging Bent- and Incumbent Party–aligned local officials for their poorly run cities, and claims that Bent is taking advantage of the cascading disaster to "rig the vote."

Thousands of accounts begin sharing audio purportedly from a conference call between the governors of the affected states, the sitting president (Incumbent candidate Bent), and Federal Emergency Management Agency officials. These false videos appear to show officials discussing the number of ballots they can collect from voters who do not show up at their polling places on Election Day. Experts are able to trace many of the original messages to foreign sources, including Russia and China, and analysis of the audio samples reveals that they were AI generated.

Meanwhile, domestic political activists take to online encrypted channels, such as Telegram, to galvanize their supporters to print and distribute flyers to homes in the affected districts, informing prospective voters that local officials have rescheduled the election for the following week as the counties resolve the ongoing water outage.

Attempts to Defend Election Integrity Meet Mixed Success

Although election officials in the affected counties quickly coordinate with other officials in their states to allow residents to vote elsewhere, they cannot assist residents who have relocated out of state. The counties are also able to fully staff existing and additional polling places with National Guard personnel, a move that prompts activist groups to call off their election-observer missions. There are anecdotal reports of people not receiving messages from county officials about their options for voting. Others learn only after the polls close that the hand-delivered flyers stating that the election had been rescheduled were inaccurate. Election turnout is significantly lower than in past general elections in the affected counties, but 10 percent of eligible voters had already received mail-in ballots by the time the cyberattacks shut down the areas' water utilities, and a few thousand from each of the heavily populated districts affected by the outage were able to vote elsewhere in their states.

As the votes are tallied, the country's attention is on the swing states that were affected by the cyberattacks because those states will decide the outcome. The election is not called for another two weeks as officials verify ballots cast outside voters' home districts. When Bent is narrowly reelected, false information about the motivation for the attacks picks up momentum. Several Challenger Party states protest the outcome by attempting to submit alternative slates of electors to disrupt the Electoral College vote, but the election is ultimately certified by Congress. Incumbent and Challenger Party supporters continue to trade accusations of blame for the disasters, and Challenger officials accuse the affected states' governors of being Challenger Party members in name only, vowing to primary them at the soonest opportunity.

Questions to Consider

This second notional scenario raises some questions for election officials, such as the following:

- How well could federal emergency management officials work together to address election security risks during an attack on critical infrastructure?
- How would state and local election officials respond to falsehoods on social media that might come from both domestic and foreign sources?
- How would state and local officials ensure confidence in U.S. election outcomes should political candidates pursue litigation about the results?

On the Scenarios

The notional examples showcase three key points. First, a single threat against one type of election security asset (i.e., physical assets) can become amplified when those assets are seemingly connected to other types of assets (i.e., human and reputational assets). Second, the realm of possible combinations of threats is large, including threats that are similar to those in past presidential elections in 2016 and 2020 (e.g., astroturf social media campaigns by foreign governments) and activities that are not as common (e.g., cyberattacks targeting public utilities). Third, AI has the potential to amplify these existing threats by making it easier to identify attack vectors for these assets and to scale and execute these attacks.

In the last section of this paper, we propose a few steps to address these potential threats in 2024.

Brokering a Shared Commitment to Free and Fair Elections

Ensuring the integrity and legitimacy of U.S. elections is vitally important for a strong and enduring democracy. Every U.S. voter, public servant, elected official, and private-sector organization has a role to play in protecting election assets from real and perceived threats. The presidential election might be contentious in 2024, as it was in 2020, but a shared understanding that free and fair elections are a fundamental right will keep the U.S. election system resilient to a perfect storm of threats.

We propose three priorities for federal officials who are responsible for protecting critical infrastructure, which extends to the U.S. election system:

- **Increase public awareness of threats and threat actors, as well as how to detect them.** To disseminate messages on social and traditional media, influence operations rely on both malicious partners and legitimate users with low levels of media literacy to erode confidence in U.S. elections. Federal agencies should enlist trusted nonpartisan partners, such as technology and cybersecurity experts, to take to these same platforms and expose these types of campaigns, explain how they function, and demonstrate how they use generative AI—including deepfakes—to amplify misleading messages and sow discord. Federal agencies will need to weigh the type of nonpartisan intervention against the need to protect First Amendment rights of users and platforms.

  Combining this public awareness with a unified approach to messaging and threat mitigation at all levels of government could be the single most important action that officials can take to defend election integrity.

  To ensure that those in power do not politicize claims of election interference, such efforts must balance a top-down approach (e.g., public awareness raised by federal authorities, such as the intelligence community) with a bottom-up approach from state and local officials. Broadening involvement across levels of stakeholders could reduce the risk that the U.S. election system is being or appears to be used to further narrow, partisan end goals. Exposing efforts might be the most effective way to warn the public. For example, during the 2020 election, the U.S. intelligence community exposed Iranian cyber actors, pretending to be members of the conservative Proud Boys group, who sent threatening emails to Democratic voters in multiple states (National Intelligence Council, 2021).
- **Take proactive measures to strengthen engagement with state, local, tribal, and territorial governments.** Monitoring and mitigating threats to the U.S. election system can be particularly challenging at the local level, where voter-registration systems could be hacked and where election workers could access or give others unauthorized access to voting equipment in 2020 (Ulmer and Layne, 2022). Human election assets—the country's election workers—are on the front line preserving democracy. Some of those who did carry out their duties lawfully in 2020 received death threats. These incidents have had a chilling effect on election-worker recruitment (Hamilton, 2022). The federal government has a responsibility to support state and local officials who are responsible for carrying out elections and provide them the resources they need to secure their voter rolls and election equipment against cyber and physical threats, as well as mis- and disinformation campaigns. The Elections Infrastructure Information Sharing and Analysis Center and the Cybersecurity and Infrastructure Security Agency's Joint Cyber Defense Collaborative are sources for training, information-sharing, and inci-

dent response support. But there could be a more coordinated effort to educate and prepare state and local officials for the threats they might encounter during the election cycle.

- **Engage in scenario-based planning to ensure a rapid and effective response to threats.** Strategic gaming methods that involve diverse stakeholders can help stakeholders prepare for unique combinations of threats targeting election assets, prioritize potential threats, and formulate strategies and interventions to prevent and mitigate risks to U.S. election infrastructure (Davenport et al., 2022; Litterer et al., 2023). The two scenarios presented here can serve as a starting point for these types of exercises, but we propose that officials collaborate with experts to develop scenarios that reflect the risk environment at the local and state levels. These exercises provide an opportunity for participants to exchange ideas, strengthen coordination, and ensure that procedures are in place before threats arise. The use of such exercises will need safeguards in place to ensure that they are transparent and truly nonpartisan in nature and that they do not intentionally or unintentionally provide advantages to any candidate over any other.

  Further evaluations are needed of how best to put these safeguards into place. Such scenario-based planning is a means for election officials to identify the constraints under which they might operate should an assortment of threats to various election assets materialize simultaneously.

Even with the above proposals, the United States is likely to face significant challenges that might not completely eliminate various perfect storms of election threats despite best efforts by local, state, and federal authorities.

To conclude, as the 2024 U.S. presidential election approaches, we anticipate not only an increase in isolated threats to election-related assets but also the conditions for a perfect storm of threats that could undermine public confidence in election outcomes at wide scale. Emerging technologies, such as AI, could exacerbate the damage from this storm. Investing in proactive measures, such as effective public awareness campaigns, engagement and coordination with officials at all levels of government, and scenario-based exercises to help these officials prepare for and respond to emerging threats, could yield significant benefits if a perfect storm materializes during the upcoming election cycle.

Notes

[1] Some of these cases were unresolved at the time of the writing of this paper in October 2023.

[2] In October 2020, RAND published a report detailing the ubiquitous presence of highly suspect Twitter accounts with the hallmarks of a Russian social media campaign designed to promote social divisions and cast aspersions on political candidates (Marcellino et al., 2020). As in the notional example in scenario 1, these findings garnered little attention from news outlets and social media users.

[3] In Ohio, voter rolls are managed at the local level. In Pennsylvania, voter rolls are managed at the state level (U.S. Election Assistance Commission, 2023).

[4] In both Ohio and Pennsylvania, a voter is allowed to cast a provisional ballot if they are not on the official roll at the precinct where they try to vote (Ohio Secretary of State, undated; Pennsylvania Department of State, undated).

References

Bond, Shannon, "Fake Viral Images of an Explosion at the Pentagon Were Probably Created by AI," *Untangling Disinformation*, National Public Radio, May 22, 2023a.

Bond, Shannon, "DeSantis Campaign Shares Apparent AI-Generated Fake Images of Trump and Fauci," *Untangling Disinformation*, National Public Radio, June 8, 2023b.

Brewster, Jack, Lorenzo Arvanitis, and McKenzie Sadeghi, "The Next Great Misinformation Superspreader: How ChatGPT Could Spread Toxic Misinformation at Unprecedented Scale," *Misinformation Monitor*, NewsGuard Technologies, January 2023.

Brumfield, Cynthia, "Why Local Governments Are a Hot Target for Cyberattacks," CSO, May 1, 2019.

Cassidy, Christina A., "Turnover Has Plagued Local Election Offices in 2020. One Swing State County Is Trying to Recover," Associated Press, October 23, 2023.

Cassidy, Christina A., and Colleen Slevin, "Voting Machine Tampering Points to Concern for Fall Election," Associated Press, August 25, 2022.

Cassidy, Christina A., and Lindsay Whitehurst, "Election Workers Have Gotten Death Threats and Warnings They Will Be Lynched, the US Government Says," Associated Press, August 31, 2023.

Collinson, Stephen, "Why Trump's Talk of a Rigged Vote Is So Dangerous," CNN, October 19, 2016.

Davenport, Aaron C., Michelle D. Ziegler, Susan A. Resetar, Scott Savitz, Katherine Anania, Melissa Bauman, and Karishma McDonald, *USCG Project Evergreen V: Compilation of Activities and Summary of Results*, RAND Corporation, RR-A872-2, 2022. As of October 10, 2023: https://www.rand.org/pubs/research_reports/RRA872-2.html

Elving, Ron, "The Florida Recount of 2000: A Nightmare That Goes on Haunting," National Public Radio, November 12, 2018.

Fabbro, Rocio, "Election Officials Combat Voter Intimidation Across U.S. as Extremist Groups Post Armed Militia at Some Polls," CNBC, November 8, 2022.

Fischer, Sara, "Exclusive: GPT-4 Readily Spouts Misinformation, Study Finds," Axios, March 21, 2023.

Freeman v. Giuliani, 2022 U.S. Dist. LEXIS 197768, D.D.C., October 31, 2022.

Fung, Katherine, "Mike Lindell Promises to 'Expose Everything' After Huge Ruling from Judge," *Newsweek*, November 21, 2023.

Hamilton, Isabelle, "US Is Facing a Poll Worker Shortage—New Campaign Hopes to Recruit Veterans to Fill the Gap," ABC News, August 12, 2022.

Helmus, Todd C., *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*, RAND Corporation, PE-A1043-1, July 2022. As of October 10, 2023:
https://www.rand.org/pubs/perspectives/PEA1043-1.html

Hodgson, Quentin E., Marygail K. Brauner, and Edward W. Chan, *Securing U.S. Elections Against Cyber Threats: Considerations for Supply Chain Risk Management*, RAND Corporation, PE-A512-1, September 2020. As of November 27, 2023:
https://www.rand.org/pubs/perspectives/PEA512-1.html

Inskeep, Steve, "Timeline: What Trump Told Supporters for Months Before They Attacked," National Public Radio, February 8, 2021.

Jaskolka, Jason, "Cyberattacks to Critical Infrastructure Threaten Our Safety and Well-Being," *The Conversation*, October 24, 2021.

Jingnan, Huo, "AI-Generated Text Is Hard to Spot. It Could Play a Big Role in the 2024 Campaign," *Untangling Disinformation*, National Public Radio, June 29, 2023.

Kavanagh, Jennifer, Quentin E. Hodgson, and C. Ben Gibson, *Do Americans Expect Safe and Secure Elections?* RAND Corporation, RR-A112-14, 2020. As of November 27, 2023:
https://www.rand.org/pubs/research_reports/RRA112-14.html

Litterer, Sydney, Jennifer Brookes, Stephen M. Worman, and David A. Shlapak, *Network Logistics Games: Design and Implementation*, RAND Corporation, RR-A470-2, 2023. As of October 10, 2023:
https://www.rand.org/pubs/research_reports/RRA470-2.html

"Machine Glitch Gave Bush Extra Ohio Votes," NBC News, November 5, 2004.

Marcellino, William, Nathan Beauchamp-Mustafaga, Amanda Kerrigan, Lev Navarre Chao, and Jackson Smith, *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI*, RAND Corporation, PE-A2679-1, September 2023. As of October 10, 2023:
https://www.rand.org/pubs/perspectives/PEA2679-1.html

Marcellino, William, Christian Johnson, Marek N. Posard, and Todd C. Helmus, *Foreign Interference in the 2020 Election: Tools for Detecting Online Election Interference*, RAND Corporation, RR-A704-2, 2020. As of October 10, 2023:
https://www.rand.org/pubs/research_reports/RRA704-2.html

McCarthy, Justin, "Confidence in Election Integrity Hides Deep Partisan Divide," Gallup, November 4, 2022.

Miller, Maggie, "Agencies Warn of Cyber Threats to Water, Wastewater Systems," *The Hill*, October 14, 2021.

Monmouth University Polling Institute, "Partisan Identity Determines Which Specific Rights Are at Risk," June 20, 2023.

National Conference of State Legislatures, "Glossary of Legislative Terms," webpage, undated. As of October 10, 2023:
https://www.ncsl.org/resources/details/glossary-of-legislative-terms

National Intelligence Council, "Foreign Threats to the 2020 US Federal Elections," Intelligence Community Assessment 2020-00078D, March 10, 2021.

Niesse, Mark, "Secret Report Finds Flaw in Georgia Voting System, but State in the Dark," *Atlanta Journal-Constitution*, January 26, 2022.

Ohio Secretary of State, "Provisional Voting," webpage, undated. As of November 29, 2023:
https://www.ohiosos.gov/elections/voters/provisional-voting/

Ortega, Bob, Audrey Ash, Curt Devine, and Scott Bronstein, "Election Deniers in Charge of Some County Election Offices Are Continuing to Sow Mistrust in the Electoral System," CNN, October 20, 2022.

Pennsylvania Department of State, "Voting by Provisional Ballot," webpage, undated. As of November 29, 2023:
https://www.vote.pa.gov/Voting-in-PA/Pages/Voting-by-Provisional-Ballot.aspx

Posard, Marek N., Marta Kepe, Hilary Reininger, James V. Marrone, Todd C. Helmus, and Jordan R. Reimer, *From Consensus to Conflict: Understanding Foreign Measures Targeting U.S. Elections*, RAND Corporation, RR-A704-1, 2020. As of October 10, 2023:
https://www.rand.org/pubs/research_reports/RRA704-1.html

Reinhart, R. J., "Faith in Elections in Relatively Short Supply in U.S.," Gallup, February 13, 2020.

Seelye, Katharine Q., "McCain's Warning About Voter Fraud Stokes a Fiery Campaign Even Further," *New York Times*, October 26, 2008.

Select Committee to Investigate the January 6th Attack on the United States Capitol, U.S. House of Representatives, *Final Report: Select Committee to Investigate the January 6th Attack on the United States Capitol*, December 22, 2022.

Shamsian, Jacob, "One America News Settles Defamation Lawsuit from a Dominion Executive at the Center of Election Conspiracy Theories," *Business Insider*, September 5, 2023.

Sullivan, Kate, "Trump Acknowledges He Was Told 2020 Election Lies Were False in Wide-Ranging Interview," CNN, September 18, 2023.

Ulmer, Alexandra, and Nathan Layne, "Trump Allies Breach U.S. Voting Systems in Search of 2020 Fraud 'Evidence,'" Reuters, April 28, 2022.

United States of America v. Donald J. Trump, indictment, D.D.C., filed August 1, 2023.

U.S. Agency for International Development, "Supporting Free and Fair Elections," webpage, undated. As of October 10, 2023: https://www.usaid.gov/democracy/supporting-free-and-fair-elections

US Dominion, Inc. v. Fox News Network, Inc., 293 A.3d 1002, 2023 Del. Super. LEXIS 161, March 31, 2023.

U.S. Election Assistance Commission, *Election Administration and Voting Survey 2022 Comprehensive Report: A Report from the U.S. Election Assistance Commission to the 118th Congress*, June 2023.

Walter, Kyle, *Testing Multimodal Generative AI: Generating Election Mis-and-Disinformation Evidence*, Logically, c. 2023.

Williams, Rhiannon, "Humans May Be More Likely to Believe Disinformation Generated by AI," *MIT Technology Review*, June 28, 2023.

Acknowledgments

We thank Shelly Culbertson for her oversight and management of this project. We thank Lauren Skrabala from RAND, whose dedicated work improved the prose of this paper. Finally, we thank Quentin Hodgson from RAND; Christian Johnson from Protect Democracy; and James Bohn, formerly of the Federal Reserve Bank of Boston, for their thoughtful reviews of this report.

About the Authors

Marek N. Posard is a military sociologist at RAND. His primary research areas include countering disinformation, security clearance vetting, and studying personnel working within military organizations. He has a Ph.D. in sociology.

Todd C. Helmus is a senior behavioral scientist at RAND. A nationally recognized expert on disinformation and violent extremism, he specializes in the use of data and evidence-based strategies to understand and counter disinformation and extremism. He has a Ph.D. in clinical psychology.

Michelle Woods is associate director of both the RAND Homeland Security Research Division and the Homeland Security Operational Analysis Center, as well as a senior defense researcher at RAND. She has an M.P.A. in management.

Bilva Chandra is a former technology and security policy fellow at RAND and now a senior artificial intelligence policy adviser for the National Institute of Standards and Technology. Her research interests are in technology safety, ethics, and national security. She has an M.A. in security studies with a technology and security concentration.

About This Paper

As the 2024 presidential election approaches, the U.S. electoral system is likely to face threats that undermine public confidence in the results. Although any single threat to the electoral system in isolation is concerning, what is more alarming is the prospect of a "perfect storm" of threats. The expanding availability of artificial intelligence tools could compound the devastation from this storm, making communication and cooperation critical for state, local, tribal, and territorial governments and federal agencies, as well as the private sector. Scenario-based planning is an approach that can help prepare these stakeholders to prevent and respond to the emerging threats to election integrity.

The purpose of this paper is to organize the key features of this perfect storm, explore how recent advances in generative artificial intelligence could accelerate the effects of this storm, and discuss next steps for policymakers and other stakeholders to consider when preparing for these threats in advance of the 2024 presidential election.

This work should be of interest to election officials within the federal, state, and local governments, as well as nongovernment stakeholders.

RAND Homeland Security Research Division

This research was sponsored by the U.S. Department of Homeland Security and conducted in the Infrastructure, Immigration, and Security Operations Program of the RAND Homeland Security Research Division (HSRD). HSRD operates the Homeland Security Operational Analysis Center, a federally funded research and development center sponsored by the U.S. Department of Homeland Security. HSRD also conducts research and analysis for other federal, state, local, tribal, territorial, and public- and private-sector organizations that make up the homeland security enterprise, within and outside the Homeland Security Operational Analysis Center contract. In addition, HSRD conducts research and analysis on homeland security matters for U.S. allies and private foundations.

For more information on HSRD, see www.rand.org/hsrd. For more information on this publication, see www.rand.org/t/PEA3073-1.